Seminar 6

Breaches

Team 3

Jonathan Ashmore




Introduction

- My assigned case study is the Marriott International breach (Fruhlinger, 2020).
- The Marriott International hotel company suffered a data breach which exposed sensitive details of its customers in 2018 (Swinhoe and Hill, 2021).

Questions

- What types of data were affected?
- What happened?
- Who was responsible?
- Where any escalations stopped?- How?
- Was the Business Continuity Plan instigated?
- Was the ICO notified?
- Were affected individuals notified?
- What were the social, legal, and ethical implications of the decision made?

- **What types of data were affected?**

➢ passport numbers, credit card details, names, DOB; gender, communication preferences, dates, and account details.

- **What happened?**

➢ Roughly 500million accounts were breached on an old reservation database. It had been going on since 2014.

- **Who was responsible?**

➢ US intelligence services believes it to be state-sponsored Chinese operatives.

- **Where any escalations stopped?- How?**

➢ An internal security tool alerted to a suspicious attempt to gain access to an internal guest reservation database. The following forensics process has not been made public.

- **Was the Business Continuity Plan instigated?**

➢ It is unknown at the moment.

- **Was the ICO notified?**

➢ The ICO fined the company £99 million reduced to £18.4 million for failing to protect UK customers' personal data secure.

- **Were affected individuals notified?**

➢ Yes, and there is a class action law suit filed by the affected individuals.

- **What were the social, legal, and ethical implications of the decision made?**

➢ It is unknown as the stolen data has not been released. It is believed the data is being secretly stored by the attackers as intelligence on US personnel. Phishing emails purported to be from Marriott asked individuals to reset passwords.

- **If you had been the ISM for Marriott International what mitigations would you have put in place to stop any reoccurrences?**

- Have defence in-depth.
- Separate encryption keys and encrypted databases.
- Regular updating of IAM protocols.
- Frequent password changes.
- Improve non-repudiation and log processes such as AWS Detective.
- Use better IDS and IPS tools.
- Use database defence tools such as Microsoft Defender for SQL.
- Isolate and segregate networks and systems.
- Conduct regular pen-tests including white and black box testing.
- Keep legacy IT and key staff when companies merge.
- Improve multifactor authentication- use key-based devices
- *Assume you have already been breached and act.*

References

Fruhlinger, J. (2020) *Marriott data breach FAQ: How did it happen and what was the impact?* CSO Online. Available from: https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html#:~:text=Marriott%20data%20breach%20FAQ%3A%20How%20did%20it%20happen [Accessed 10 May 2022].

Swinhoe, D. and Hill, M. (2021). *The 18 biggest data breaches of the 21st century*. CSO Online. Available from: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html [Accessed 10 May 2022].